AMENDMENTS TO THE SPECIFICATION

Please replace Paragraph [0037] with the following paragraph rewritten in amendment format:

[0037] ~~The object of the invention is achieved by a~~A digital certificate issuing system with intrusion tolerance ability, comprising: at least one online task distributor, sending out a certificate to be signed through a first broadcast channel; k online secret share calculators, each receiving the certificate to be signed, checking correctness of the certificate to be signed, making calculation based on first sub-secret-keys pre-stored, and sending out a calculation result through a second broadcast channel; m online secret share combiners, each receiving the calculation results from the online secret share calculators, comparing t calculation results with the equation combination representations pre-stored upon receiving at least t calculation results to get a second sub-secret-key corresponding to the t calculation results, making a calculation based on the t calculation results and the second sub-secret-key corresponding to the t calculation results, and generating a digital certificate; an offline secret key distributor, pre-storing the first sub-secret-keys in each of the online secret share calculators, and pre-storing the second sub-secret-keys and equation combination representations thereof in each of the online secret share combiners during a system initialization or configuration process; and the k, m, t are positive integers, and the t is less than the k. ~~at least one online task distributor, k online secret share calculators, m online secret share combiners and an offline secret key distributor; said online task distributor is connected to said k secret share calculators through a first broadcast channel, said k secret share calculators are connected to said m secret share~~

~~combiners through a second broadcast channel; said offline secret key distributor is connected to said k secret share calculators and m secret share combiners during system initialization or configuration process; wherein k and m are positive integers~~

Please replace Paragraph [0041] with the following paragraph rewritten in amendment format:

[0041] Wherein distributing the signing private key of a CA comprises:

A. setting a digital certificate issuing mechanism which comprises an online task distributor, k online secret share calculators, m online secret share combiners, broadcast channels and an offline secret key distributor, wherein k and m are positive integers;

B. said offline secret key distributor expressing the signing private key d as a sum of t first sub-secret-keys dji and a second sub-secret-key ~~ca~~c_a; wherein d, t, c, j, i and a all are positive integers, t < k, j is the machine number of the jth secret share calculator, i is the first sub-secret-key number inside the machine of the secret share calculators, a is the second sub-secret-key number inside the machine of the secret share combiner, j = 1, 2 … k, and i = 1, 2 … l;

C. said offline secret key distributor generates k×l random positive integers as the first sub-secret-keys d_{ji} ~~dji~~ and distributing them to k secret share calculators so that each secret share calculator stores l first sub-secret-keys d_{ji}~~dji~~; based on the additive relation between t first sub-secret-keys and one second sub-secret-key in Step B, obtaining second sub-secret-keys c_a~~ca~~ and their equation combination representations by subtracting; and then obtaining their equivalent combination sets from the equation combination representations and putting them into a large group;

D. according to combiner security condition, said offline secret key distributor making exhaustive search for all equivalent combination sets in said large group and taking one equation combination representation from each equivalent combination set as a representative; putting all representatives of equivalent combination sets into m subgroups, obtaining the second sub-secret-keys C_a~~ea~~ and their equation combination representations of the m subgroups;

E. said offline secret key distributor sending second sub-secret-keys C_a~~ea~~ and their equation combination representations of the m subgroups to m secret share combiners for pre-storage;

Please replace Paragraph [0042] with the following paragraph rewritten in amendment format:

[0042] The process of computing digital signature for a certificate comprises:

F. said online task distributor sending said certificate to be signed and its hash value M to said k secret share calculators via the first broadcast channel through broadcasting data packets;

G. t or more than t secret share calculators among k secret share calculators checking correctness of said certificate to be signed based on the received certificate and its hash value M, and then making ascending power computation $M^{d_{ji}}$; sending secret share calculators number j, said processed certificate and its hash value M, the secret key number i inside the secret share calculators and I computation results $M^{d_{ji}}$

to m secret share combiners via the second broadcast channel through broadcasting data packets;

H. said m secret share combiners checking the received results, and then comparing the received results with pre-stored equivalent combination representations of the second sub-secret-keys c_a~~ca~~ and finding out a matching equivalent combination representation and the corresponding second sub-secret-key c_a~~ca~~, and then checking correctness of said certificate to be signed; after that, to obtain R by multiplying ascending power computation results of t secret share calculators matching to the combination; finally, computing M^{c_a} based on the found c_a~~ca~~, and multiplying M^{c_a} with R to obtain a digital signature S=M^d~~Md~~;

I. generating a certificate based on said digital signature and the content of said certificate to be signed.

Please replace Paragraph [0044] with the following paragraph rewritten in amendment format:

[0044] Preferably, Step C further comprising:

c1. said offline secret key distributor generating k×l random positive integers as first sub-secret-keys d_{ji}~~dji~~ and sending them to k secret share calculators with a mode accepted by administration;

c2. said offline secret key distributor solving all equation combination representations from combination formula C_k^t, extending each equation combination representation to solve its equivalent combination set; wherein each equivalent combination set has $\underline{l}^t$~~lt~~ combinations and each combination has t items consisted of two digits ~~j~~$\underline{\text{j and}}$ i; and

c3. putting all equivalent combination sets into a big group

Please replace Paragraph [0054] with the following paragraph rewritten in amendment format:

[0054] The method and system according to the invention have the following characteristics:

1. The online task distributor can broadcast a digital signature task without selecting secret share calculators and specifying sub-secret-keys, so when system is updating, the online task distributor will not be affected, and when a secret share calculator is damaged suddenly, execution time for broadcasting a task will not be affected too.

2. When adding a secret share calculator, it is necessary only to generate a set of first sub-secret-keys for the new secret share calculator. The offline secret-key distributor can make equation combination according to the number of the newly added secret share calculator and the numbers of existing secret share calculators, compute the corresponding second sub-secret-key $\underline{C_a}$~~ea~~, and then add the new equation combination representation and $\underline{C_a}$~~ea~~ to the secret share combiner in a way accepted by administration. The adding will not affect the system normal operation.

3. When taking away a secret share calculator, shutting down the device is enough; for efficiency reason, equation combination representation including the secret share calculator number and corresponding $\underline{C_a}$~~ea~~ can be deleted.

4. The invention has the intrusion tolerance ability as other schemes mentioned in background section. When less than t secret share calculators are intruded, the system secret key d will not be leaked. Since secret share combiners are added, even all secret share calculators are intruded, the system secret key d will not be leaked also. It can be proved theoretically that attacking secret share combiners cannot obtain the system secret key d; although there are many equations, the rank of coefficient matrix of the equations is less than the number of variables.

5. The invention can resist a conspiracy attack from the secret share calculator and the secret share combiner, i.e. even when a conspiracy attack is done by a secret share calculator and a secret share combiners, the system secret key d will not be leaked, furthermore, comparing with other schemes, the number of the secret share combiners can be less greatly, for example, when k = 5 and t = 3, the least number of secret share combiners is 2.

6. An operator confirmation is added during distributing private key and issuing certificate, which will further guarantee security and reliability of issuing digital certificate. Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention

Please replace Paragraph [0064] with the following paragraph rewritten in amendment format:

[0064] The processing of sharing secret d in this system structure is completed through two layers of components: one layer of components are composed of secret share calculators 23 and another layer of components are composed of secret share combiners 24. More than one d_{ji} are respectively stored in the secret share calculators 23, and c_a is stored in the secret share combiners 24. In this way, a two-layer secret share structure is formed. Two layers of components respectively store first sub-secret-key d_{ji} and second sub-secret-key c_a. The first sub-secret-key d_{ji} employs two digits as its suffix, among them the first digit j is a sequence number, i.e. device number, of the secret share calculators 23, j = 1, 2 … k, and the second digit i is a number of the secret keys stored in a certain secret share calculator 23, i = 1, 2 … I. For example, when a secret share calculator 23 stores two items of d_{ji}, the first sub-secret-key respectively are d_{j1} and d_{j2}, meanwhile d_{11} and d_{12} represent two items of first sub-secret-keys stored in the first secret share calculator. The a is the second sub-secret-key number inside the machine of the secret share combiner.